

**UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF TEXAS  
MARSHALL DIVISION**

K.MIZRA LLC,

Plaintiff,

v.

HEWLETT PACKARD ENTERPRISE  
COMPANY and ARUBA NETWORKS,  
LLC,

Defendants.

Civil Action No. 2:21-cv-305

**JURY TRIAL DEMANDED**

**HEWLETT PACKARD ENTERPRISE COMPANY AND ARUBA NETWORKS, LLC'S  
ANSWER TO K.MIZRA LLC'S COMPLAINT**

Defendants Hewlett Packard Enterprise Company ("HPE") and Aruba Networks, LLC ("Aruba") (collectively, "Defendants") for their Answer to Plaintiff K.Mizra LLC's ("K.Mizra" "Plaintiff") Complaint, state the following:

1. This is an action for the infringement of U.S. Patent Nos. 8,234,705 ("the '705 patent") and 9,516,048 ("the '048 patent"), also referred to as "the Patents-in-Suit."

**ANSWER:** Defendants admit that this is an action alleging infringement of U.S. Patent Nos. 8,234,705 ("the '705 patent") and 9,516,048 ("the '048 patent"). Defendants deny that they have infringed either patent.

2. Defendant Aruba has been making, selling, using, and offering for sale computer network security products and services such as the ClearPass Policy Manager<sup>1</sup>, ClearPass OnGuard<sup>2</sup> and equipment, including HPE Aruba Appliances (*e.g.*, the C1000, C2010, and C3010)<sup>3</sup>,

---

<sup>1</sup> See Exhibit C, Data Sheet HPE Aruba ClearPass Policy Manager at 1 (available at [https://www.arubanetworks.com/assets/ds/DS\\_ClearPass\\_PolicyManager.pdf](https://www.arubanetworks.com/assets/ds/DS_ClearPass_PolicyManager.pdf), last visited July 8, 2021).

<sup>2</sup> See Exhibit D, Data Sheet HPE Aruba ClearPass OnGuard at 1 (available at [https://www.arubanetworks.com/assets/ds/DS\\_ClearPass\\_OnGuard.pdf](https://www.arubanetworks.com/assets/ds/DS_ClearPass_OnGuard.pdf), last visited July 8, 2021).

<sup>3</sup> See Exhibit C, Data Sheet HPE Aruba ClearPass Policy Manager at 4.

and software, including virtual appliances<sup>4</sup>, incorporating similar technology that infringe the '705 and '048 patents in violation of 35 U.S.C. § 271 (collectively, "the Accused Instrumentalities").

**ANSWER:** Defendants admit that Aruba sells certain computer network security products and services. Defendants deny that they have infringed either the '705 or '048 patent and deny the remaining allegations in Paragraph 2.

3. Plaintiff K.Mizra seeks appropriate damages and prejudgment and post-judgment interest for Defendants' infringement of the Patents-in-Suit.

**ANSWER:** Defendants deny that they have infringed the Patents-in-Suit. Defendants lack sufficient information to admit or deny the remaining allegations in this Paragraph and, therefore, deny the same.

4. Plaintiff K.Mizra is a Delaware limited liability company with its principal place of business at 777 Brickell Ave, #500-96031, Miami, FL 33131. K.Mizra is the assignee and owner of the Patents-in-Suit.

**ANSWER:** Defendants lack sufficient information to admit or deny the allegations in this Paragraph and, therefore, deny the same.

5. Defendant Hewlett Packard Enterprise Company is a Delaware Corporation that maintains regular and established places of business throughout Texas, for example, at its facilities at 6080 Tennyson Parkway, Suite 400, Plano, TX 75024. HPE is registered to conduct business in the state of Texas and has appointed CT Corporation System, located at 1999 Bryan ST., Ste. 900, Dallas, TX 75201 as its agent for service of process.

**ANSWER:** Defendants admit that HPE is a Delaware Corporation. Defendants admit that HPE has a business office located at 6080 Tennyson Parkway, Suite 400, Plano, TX 75024. Defendants further admit that HPE is registered to do business in Texas and that CT Corporation System is HPE's registered agent for service of process in Texas. Defendants deny the remaining allegations of this Paragraph.

---

<sup>4</sup> See id.

6. By maintaining facilities in Plano, HPE has a regular and established place of business in the Eastern District of Texas.

**ANSWER:** To the extent the allegations of this Paragraph purport to state a legal conclusion, no response thereto is required. To the extent that a response is deemed to be required, Defendants admit that HPE has a place of business in the Eastern District of Texas and deny the remaining allegations in this Paragraph.

7. Defendant Aruba Networks, LLC is a Delaware limited liability company with its principal place of business at 6280 America Center Drive, San Jose, CA 95002. Aruba is registered to conduct business in the state of Texas and has appointed CT Corporation System, located at 1999 Bryan ST., Ste. 900, Dallas, TX 75201 as its agent for service of process.

**ANSWER:** Admitted.

8. Defendant Aruba Networks, LLC. is a wholly owned subsidiary of Defendant Hewlett Packard Enterprise Company. Defendants conduct business operations within the Eastern District of Texas where they sell, develop, and or market their products, including facilities at 6080 Tennyson Parkway, Suite 400, Plano, TX 75024.

**ANSWER:** Defendants admit that Aruba is a wholly owned subsidiary of HPE. Defendants admit that HPE has a business office located in the Eastern District of Texas at 6080 Tennyson Parkway in Plano, Texas. Defendants deny that Aruba has a business office located in the Eastern District of Texas. Defendants deny the remaining allegations in this Paragraph.

9. Defendants have been aware of the '705 patent and their infringement of the patent at least as of January 2021, when K.Mizra provided a claim chart of the '705 patent to Defendants during an exchange of emails between K.Mizra's principal and HPE's in-house litigation counsel.

**ANSWER:** Denied.

10. In early January 2021, K.Mizra sent letters to HPE and Aruba inviting them to discuss their products' infringement of K.Mizra's patents and potentially taking a license to K.Mizra's patent portfolio. Shortly thereafter, HPE responded to the letters by email, at which time K.Mizra provided a preliminary claim chart demonstrating Defendants' infringement of the '705 patent. To date, however, HPE and Aruba have not taken a license to K.Mizra's patents.

**ANSWER:** Denied.

11. Notwithstanding their receipt of notice that the Accused Instrumentalities infringe the '705 patent in January 2021, Defendants continue to sell the Accused Instrumentalities in flagrant disregard of K.Mizra's rights under the Patents-in-Suit.

**ANSWER:** Denied.

12. This is an action for patent infringement arising under the Patent Laws of the United States, Title 35 of the United States Code.

**ANSWER:** Defendants admit that this is an action alleging patent infringement. Defendants deny that they have infringed either Patent-in-Suit.

13. This Court has original subject matter jurisdiction under 28 U.S.C. §§ 1331 and 1338(a).

**ANSWER:** To the extent the allegations of this Paragraph purport to state a legal conclusion, no response thereto is required. To the extent that a response is deemed to be required, Defendants admit that the Court has jurisdiction over claims for patent infringement under 28 U.S.C. §§ 1331 and 1338(a).

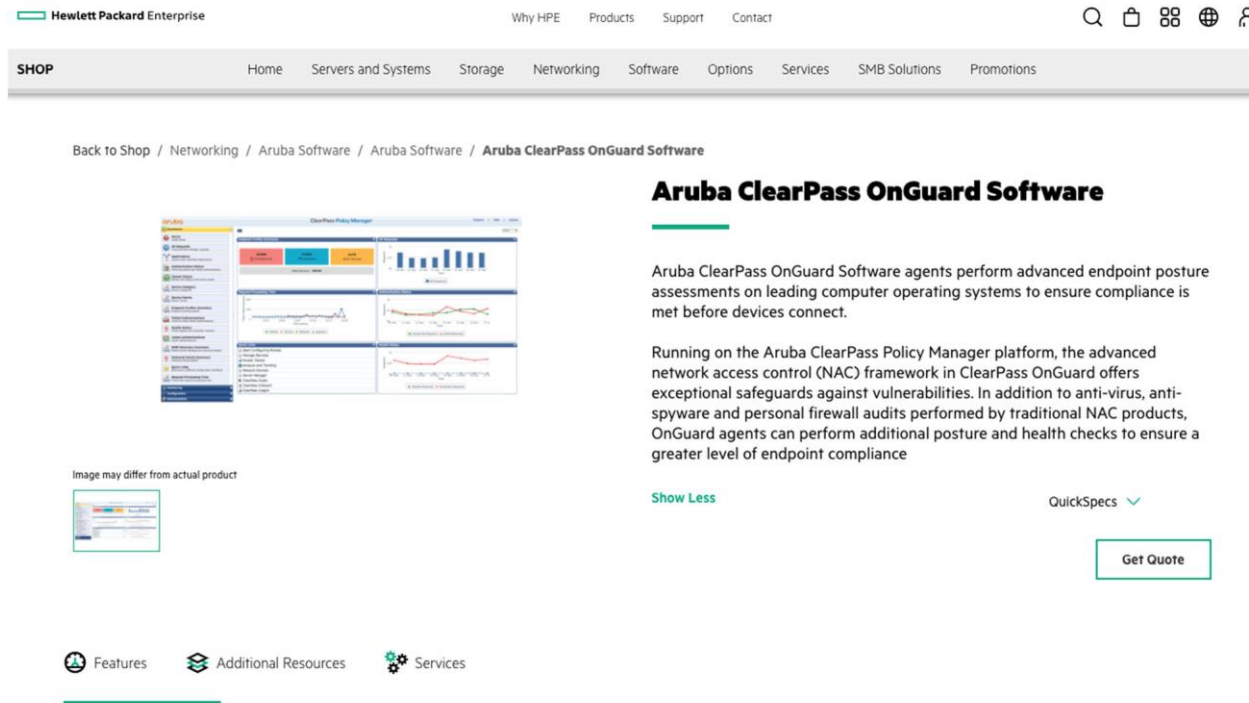
14. This Court has personal jurisdiction over Defendants because, *inter alia*, Defendants have a continuous presence in, and systematic contact with, this District and have registered to conduct business in the state of Texas.

**ANSWER:** To the extent the allegations of this Paragraph state a legal conclusion, no response thereto is required. To the extent a response is deemed to be required, Defendants do not challenge that this Court has personal jurisdiction over them for purposes this action. Defendants further admit that HPE is registered to conduct business in the state of Texas. Defendants admit that Aruba is registered to conduct business in the state of Texas, but deny that Aruba has a continuous presence in or systematic contact with this District.

15. Defendants have committed and continue to commit acts of infringement of K.Mizra's Patents-in-Suit in violation of the United States Patent Laws, and have made, used, sold, offered for sale, marketed and/or imported infringing products into this District. Defendants' infringement has caused substantial injury to K.Mizra, including within this District.

**ANSWER:** Denied.

16. Defendant HPE does not simply act as a wholly separate parent of Aruba. HPE offers for sale infringing Aruba products on the HPE website, soliciting sales of infringing products by consumers in this District and in the state of Texas. For example, HPE offers for sale Aruba ClearPass OnGuard products which infringe the Patents-in-Suit, on its website:



See <https://buy.hpe.com/us/en/networking/aruba-software/aruba-software/aruba-wireless-software/aruba-clearpass-onguard-software/p/1009648564> (last visited August 9, 2021).

**ANSWER:** Defendants deny that they have infringed either Patent-in-Suit. Defendants admit that HPE offers for sale Aruba ClearPass OnGuard products. Defendants deny the remaining allegations of this Paragraph.

17. Moreover, HPE and Aruba regularly identify their products using both Defendants' branding. For example, Defendants offer for sale infringing products with model names such as "Aruba ClearPass," "HPE DL20 Gen10," and "HPE DL360 Gen10."

DATA SHEET  
ARUBA CLEARPASS POLICY MANAGER



	C1000 Appliance (JZ508A)	C2010 Appliance (R1V81A)	C3010 Appliance (R1V82A)
<b>APPLIANCE SPECIFICATIONS</b>			
Hardware Model	Unicom S-1200 R4	HPE DL20 Gen10	HPE DL360 Gen10
CPU	(1) Atom 2.4GHz C2758 with Eight Cores (8 Threads)	(1) Xeon 4.0GHz E-2274G with Four Cores (8 Threads)	(1) Xeon 2.3GHz Gold 5118 with Twelve Cores (24 Threads)
Memory	8 GB	16 GB	64 GB
Hard drive storage	(1) SATA (7.2K RPM) 1TB hard drive	(2) SATA (7.2K RPM) 1TB hard drives, RAID-1 controller	(6) SAS (10K RPM) 600GB Hot-Plug hard drives RAID-10 controller
Out of Band Management	N/A	HPE Integrated Lights-Out (iLO)	HPE Integrated Lights-Out (iLO) Advanced
Network Interface	4 x 1GbE	4 x 1GbE	4 x 1GbE

See Exhibit C, Data Sheet HPE Aruba ClearPass Policy Manager at 4.

**ANSWER:** Denied.

18. HPE also offers services for infringing Aruba ClearPass products on the HPE website. For example, HPE sells hardware and software services as well as advisory and professional services for the Aruba ClearPass products including service planning, system design, deployment, and integration, and project management for its customers.



Data sheet

## ARUBA CLEARPASS SERVICES

### Advisory and Professional Services from HPE Pointnext Services

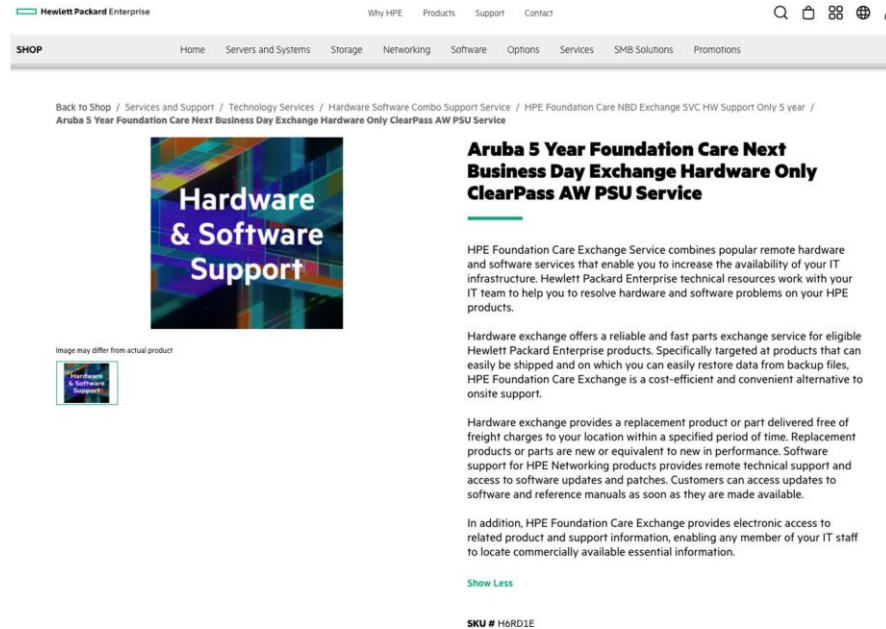
Aruba ClearPass Services from HPE for wired and wireless local area networks (WLANs) provide you with access to Aruba Mobile First technology expertise to help enable pervasive wireless infrastructures with security features that can support communication in a wide range of locations and deliver business apps wherever people work. These services are an integral part of a family of Aruba Mobile First services that are designed to help you support reliable bring your own (BYO) everything connectivity while also helping to simplify the day-to-day operation of managing a more secure and flexible infrastructure.

Aruba ClearPass Services focus on the lifecycle of Advisory and Professional Services needed to help implement Aruba ClearPass network access security features for your indoor, outdoor, public, and private enterprise networks. Depending on your specific access requirements, these services can include:

- Predeployment strategy, product, and service planning to help you prepare for your wired and wireless LAN security project
- A wired and wireless LAN access assessment of existing security mechanisms
- Design of a network with ClearPass security features that are aligned to mobile application and unified wired and wireless security strategies
- Implementing Aruba ClearPass Policy Manager to help IT to manage network access security and policy enforcement
- A knowledge transfer session for your IT team to help them take ownership of the new wired/wireless network and HPE security related best practices
- End-to-end program management and the HPE Trusted Network Transformation approach and methodology designed to help you to manage costs while delivering the kind of pervasive, flexible (BYO anything) wireless connectivity that you want

The service features in Table 1 provides information on the service features available under these network Advisory and Professional Services. The specific service features provided will be custom priced and scoped in a mutually agreed and executed statement of work (SOW) based upon the customer's requirements.

See <https://www.hpe.com/psnow/doc/4aa6-2768enw> (last visited August 9, 2021).



See <https://buy.hpe.com/us/en/services-support/technology-services/hardware-software-combo-support-service/hpe-foundation-care-exchange-service-hw-support-only/hpe-foundation-care-nbd-exchange-svc-hw-support-only-5-year/aruba-5-year-foundation-care-next-business-day-exchange-hardware-only-clearpass-aw-psu-service/p/H6RD1E> (last visited August 9, 2021).

**ANSWER:** Defendants deny that they have infringed either Patent-in-Suit. Defendants admit that they offer services related to Aruba ClearPass OnGuard products on the HPE website. Defendants deny the remaining allegations of this Paragraph.

19. Venue is proper in this District pursuant to 28 U.S.C. §§ 1400 and 1391 because Defendants have committed acts of infringement in this District and maintains a regular and established place of business in this District.

**ANSWER:** To the extent the allegations of this Paragraph purport to state a legal conclusion, no response thereto is required. To the extent that a response is deemed to be required, Defendants do not contest that they are subject to venue in this District for purposes of this litigation only. Defendants each expressly reserve the right to contest venue in any other case as to any party. Defendants deny that Aruba maintains a regular and established place of business in this District. Defendants deny the remaining allegations in this Paragraph.

**THE PATENTS-IN-SUIT**

20. The '705 patent is titled "Contagion Isolation and Inoculation" and was issued by the United States Patent Office to inventors James A. Roskind and Aaron R. Emigh on July 31, 2012. The earliest application related to the '705 patent was filed on September 27, 2004. A true and correct copy of the '705 patent is attached as Exhibit A.

**ANSWER:** Defendants admit that the '705 Patent issued on July 31, 2012, and is entitled "Contagion Isolation and Inoculation." Defendants deny that the '705 Patent was duly and legally issued. Defendants further admit that what purports to be a copy of the '705 Patent is attached as Exhibit A to the Complaint. Defendants deny the remaining allegations of this Paragraph.

21. K.Mizra is the owner of all right, title and interest in and to the '705 patent with the full and exclusive right to bring suit to enforce the '705 patent.

**ANSWER:** Defendants lack sufficient information to admit or deny the allegations in this Paragraph and, therefore, deny the same.

22. The '705 patent is valid and enforceable under the United States Patent Laws.

**ANSWER:** Denied.

23. The '048 patent is titled "Contagion Isolation and Inoculation Via Quarantine" and was issued by the United States Patent Office to inventors Aaron R. Emigh and James A. Roskind on December 6, 2016. The earliest application related to the '048 patent was filed on September 27, 2004. A true and correct copy of the '048 patent is attached as Exhibit B.

**ANSWER:** Defendants admit that the '048 Patent issued on December 6, 2016, and is entitled "Contagion Isolation and Inoculation Via Quarantine." Defendants deny that the '048 Patent was duly and legally issued. Defendants further admit that what purports to be a copy of the '048 Patent is attached as Exhibit B to the Complaint. Defendants deny the remaining allegations of this Paragraph.

24. K.Mizra is the owner of all right, title and interest in and to the '048 patent with the full and exclusive right to bring suit to enforce the '048 patent.

**ANSWER:** Defendants lack sufficient information to admit or deny the allegations in this Paragraph and, therefore, deny the same.

25. The '048 patent is valid and enforceable under the United States Patent Laws.

**ANSWER:** Denied.

26. The claims of the '705 and '048 patents are directed to technological solutions that address specific challenges grounded in computer network security. The security of computer systems and networks is a tremendous concern for modern enterprises, since a breach of an internal network can have severe repercussions, including major financial losses, data theft, disclosure of sensitive information, network disruptions, and data corruption—any of which could have devastating consequences to a business, at any scale. The inventors of the '705 and '048 patents understood that while a network security appliance or hardware can be adept at keeping out unwanted external intrusions into the network, the most exploitable vulnerabilities of a computer network are the end-user computers that roam throughout various other public and private network domains and then access the presumably secure network day in and day out.

**ANSWER:** Defendants lack sufficient information to admit or deny the allegations in this Paragraph and, therefore, deny the same.

27. For example, the '705 patent explains that “[l]aptop and wireless computers and other mobile systems pose a threat to elements comprising and/or connected to a network service provider, enterprise, or other protected networks to which they reconnect after a period of connection to one or more networks and/or systems that are not part of the service provider, enterprise, or other protected network. By roaming to unknown domains, such as the Internet, and/or connecting to such domains through public, wireless, and/or otherwise less secure access nodes, such mobile systems may become infected by computer viruses, worms, backdoors, and/or countless other threats and/or exploits and/or have unauthorized software installed; have software installed on the mobile system by an operator of the protected network for the protection of the mobile system and/or the protected network removed or altered without authorization; and/or have configurations, settings, security data, and/or other data added, removed, and/or changed in unauthorized ways and/or by unauthorized person.” *See*, e.g., Exhibit A at 1:14-31.

**ANSWER:** Defendants admit that the quoted text in Paragraph 27 appears in the '705 Patent. Defendants lack sufficient information to admit or deny the remaining allegations in this Paragraph and, therefore, deny the same.

28. While Information Technology (IT) engineers may have been able to keep on-site systems secure and up to date with the technology available at that time, they still faced challenges with off-site devices such as a worker's personal laptop or mobile device which posed significant security risks that could allow attackers or viruses stealth access into a business's network, bypassing IT security measures. For example, the '705 patent states that "[u]pon connecting to a protected network, a system may infect or otherwise harm resources associated with the protected network before measures can be taken to detect and prevent the spread of such infections or harm." *See, e.g., Exhibit A at 1:34-38.*

**ANSWER:** Defendants admit that the quoted text in Paragraph 28 appears in the '705 Patent.

Defendants lack sufficient information to admit or deny the remaining allegations in this Paragraph and, therefore, deny the same.

29. The invention of the '705 and '048 patents close this loophole by verifying that any device attempting to access a company's network meets the company's standards for network security and will not introduce dangerous computer programs or viruses into the company's network. For example, the '705 patent describes that when "a request is received from a host, e.g., via a network interface, to connect to a protected network, it is determined whether the host is required to be quarantined. According to the '705 and '048 patents, if the host is required to be quarantined, the host is provided only limited access to the protected network. *See, e.g., Exhibit A at 3:13-20, Exhibit B at 11:58-66.* In some embodiments, a quarantined host is permitted to access the protected network only as required to remedy a condition that caused the quarantine to be imposed, such as to download a software patch, update, or definition; install, remove, and/or configure software and/or settings as required by a policy; and/or to have a scan or other diagnostic and/or remedial operation performed." *See Exhibit A at 3:8-20, Exhibit B at 12:21-28.* The '705 and '048 patents further describe that "attempts to communicate with hosts not involved in remediation are redirected to a quarantine system, such as a server, that provides information, notices, updates, and/or instructions to the user." *Exhibit A at 3:20-23, Exhibit B at 12:28-33.*

**ANSWER:** Defendants admit that the quoted text in Paragraph 29 appears in the '705 and '048

Patents. Defendants lack sufficient information to admit or deny the remaining allegations in this Paragraph and, therefore, deny the same.

30. The '705 and '048 patents disclose an improvement in computer functionality related to computer network security. For instance, an infected host computer with malicious code, such as a computer virus, worm, exploits and the like ("malware"), poses a serious threat if the malware spreads to other hosts in a protected network. *Exhibit A at 1:14-41, Exhibit B at 1:42-46.* The claims of the '705 and '048 patents employ techniques, unknown at the time of the invention, that do more than detect malware per se. The claimed techniques quarantine an infected host to prevent it from spreading malware to other hosts while still permitting limited communications with the network to remedy the malware. As a result, the '705 and '048 patents provide a

technological solution to a problem rooted in computer technology by improving the way networks are secured. Through the implementation and provision of this technology by network security companies such as K.Mizra, businesses are able to increase their security from vulnerable elements that access their networks.

**ANSWER:** Defendants lack sufficient information to admit or deny the allegations in this Paragraph and, therefore, deny the same.

31. The claims of the '705 and '048 patents address the technological problems not by a mere nominal application of a generic computer to practice the invention, but by carrying out particular improvements to computerized network security technology in order to overcome problems specifically grounded in the field of computer network security. As the '705 and '048 patents explain, determining whether a quarantine is required involves detection by a computing device, router, firewall, or other network component as to the infestation or cleanliness of a computer. Exhibit A at 11:15-28, Exhibit B at 11:35-49. Moreover, the subsequent steps such as quarantining, limiting network access, remediation, and redirecting network communications are functions fundamentally rooted in computer network technology.

**ANSWER:** Defendants lack sufficient information to admit or deny the allegations in this Paragraph and, therefore, deny the same.

32. The claims of the '705 and '048 patents recite subject matter that is not merely the routine or conventional use of computer network security that existed in the prior art. Instead, the claimed inventions are directed to particularized implementations of assessing and responding to an external network access request in a way that protects the computer network and systems from malicious or undesired breaches. The claims of the '705 and '048 patents specify how a secure network can assess and respond to an external network access request without jeopardizing network integrity.

**ANSWER:** Defendants lack sufficient information to admit or deny the allegations in this Paragraph and, therefore, deny the same.

33. K.Mizra re-alleges and incorporates by reference all of the foregoing paragraphs.

**ANSWER:** Defendants incorporate by reference their answers to Paragraphs 1 through 32 as if fully set forth herein.

34. On information and belief, Aruba has infringed and continues to infringe, either literally or under the doctrine of equivalents, one or more claims, including at least claim 19, of the '705 patent in violation of 35 U.S.C. §§ 271 et seq., by making, using, importing, selling,

offering for sale, and/or importing in this District and into the United States certain products including, but not limited to those, relating to the Accused Instrumentalities.

**ANSWER:** Denied.

35. For example, Claim 19 of the '705 patent recites the following:

[preamble] A computer program product for protecting a network, the computer program product being embodied in a non-transitory computer readable medium and comprising instructions for:

[A] detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network,

[B] wherein detecting the insecure condition includes:

[B1] contacting a trusted computing base associated with a trusted platform module within the first host,

[B2] receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness,

[C] wherein the valid digitally signed attestation of cleanliness includes at least one of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host;

[D] when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network,

[E] wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes

[E1] receiving a service request sent by the first host, serving a quarantine notification page to the first host when the service request comprises a web server request,

[E2] and in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server configured to serve the quarantine notification page if a host name that is the subject of the DNS query is not

associated with a remediation host configured to provide data usable to remedy the insecure condition; and

[F] permitting the first host to communicate with the remediation host.

**ANSWER:** Denied.

36. On information and belief, and based on publicly available information, the Accused Instrumentalities satisfy each and every limitation of at least claim 19 of the ‘705 patent.

**ANSWER:** Denied.

37. Regarding the preamble of claim 19, to the extent the preamble is determined to be limiting, the Accused Instrumentalities provide the features described in the preamble, which recites a “computer program product for protecting a network.” For example, Aruba touts that “ClearPass is unrivaled as a foundation for network security for organizations of any size.” *See* Exhibit C, Data Sheet HPE Aruba ClearPass Policy Manager at 1. Specifically, the ClearPass Policy Manager provides device-based secure network access control (NAC). *See id.* HPE Aruba promotes the ClearPass Policy Manager as the most advanced Secure NAC platform available:

*See id.* Additionally, ClearPass OnGuard delivers endpoint posture assessments and ensures that endpoints meet security and compliance policies before they connect to the network:

#### DATA SHEET

### CLEARPASS ONGUARD

Enterprise-class endpoint protection, posture assessments and health checks

ClearPass OnGuard performs advanced endpoint posture assessments to ensure security and compliance requirements are met prior to devices connecting to the corporate network.

As a key component of the Aruba ClearPass Policy Manager platform, the advanced network access control (NAC) framework in ClearPass OnGuard offers exceptional safeguards against vulnerabilities.

*See, e.g.,* Exhibit C, Data Sheet HPE Aruba ClearPass Policy Manager at 2; Exhibit D, Data Sheet HPE Aruba ClearPass OnGuard at 1. Accordingly, to the extent the preamble of claim 19 is limiting, the Accused Instrumentalities meet it.

**ANSWER:** Defendants admit that the text “computer program product for protecting a network” appears in claim 19 of the ’705 Patent. Defendants admit that the text “ClearPass is unrivaled as a foundation for network security for organizations of any size” appears in Exhibit C attached to the Complaint. Defendants lack sufficient information to admit or deny the remaining allegations in this Paragraph and, therefore, deny the same.

38. Limitation A requires “detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network.” The Accused Instrumentalities also meet all the requirements of limitation A of claim 19. For example, ClearPass OnGuard delivers endpoint posture assessments and ensures that endpoints meet security and compliance policies before they connect to the network:

#### DATA SHEET

### CLEARPASS ONGUARD

Enterprise-class endpoint protection, posture assessments and health checks

ClearPass OnGuard performs advanced endpoint posture assessments to ensure security and compliance requirements are met prior to devices connecting to the corporate network.

As a key component of the Aruba ClearPass Policy Manager platform, the advanced network access control (NAC) framework in ClearPass OnGuard offers exceptional safeguards against vulnerabilities.

*See, e.g.,* Exhibit C, Data Sheet HPE Aruba ClearPass Policy Manager at 2; Exhibit D, Data Sheet HPE Aruba ClearPass OnGuard at 1. Accordingly, the Accused Instrumentalities meet limitation A of claim 19.

**ANSWER:** Defendants admit that the text “detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network” appears in claim 19 of the ’705 Patent. Defendants admit that the screenshotted image appears in Exhibit D attached to the Complaint. Defendants lack sufficient information to admit or deny the remaining allegations in this Paragraph and, therefore, deny the same.

39. Limitation B1 requires that “detecting the insecure condition includes” “contacting a trusted computing base associated with a trusted platform module within the first host.” The Accused Instrumentalities also meet all the requirements of limitation B1 of claim 19. For example, ClearPass OnGuard has multiple components, such as a user interface Frontend as well as a Backend Service. *See* Exhibit E, ClearPass OnGuard Troubleshooting at 4 (available at <https://community.arubanetworks.com/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=0e85052b-4274-4d8b-93b0-ac4872b5042a>, last visited July 8, 2021). Moreover, a ClearPass OnGuard Plugin provides health check related functionality to the Frontend and communicates with the Backend Service and the CPPM (ClearPass Policy Management) Server. *See id.* at 6. The OnGuard Plugin uses https to communicate with the CPPM (ClearPass Policy Management) Server. *See id.* at 7.

**ANSWER:** Defendants admit that the text “detecting the insecure condition includes” and “contacting a trusted computing base associated with a trusted platform module within the first host” appears in claim 19 of the ’705 Patent. Defendants lack sufficient information to admit or deny the remaining allegations in this Paragraph and, therefore, deny the same.

40. Additionally, when the OnGuard agent uses client certificates during the SSL handshake, the private key can be obtained from several sources, including a TPM:

#### **Certificate-Based Authentication Using OnGuard**

For certificate-based authentication, OnGuard agent uses the client certificate during the SSL handshake (the private key can be obtained from OS store/TPM/smart card). The ClearPass server verifies the client certificate against the configured trusted CA list.

*See* Exhibit F, “OnGuard Settings and Agent Library Updates” (available at [https://www.arubanetworks.com/techdocs/ClearPass/6.8/PolicyManager/Content/CPPM\\_UserGuide/Admin/OnGuard\\_settings.html](https://www.arubanetworks.com/techdocs/ClearPass/6.8/PolicyManager/Content/CPPM_UserGuide/Admin/OnGuard_settings.html), last visited July 8, 2021).

**ANSWER:** Defendants admit that the screenshotted image appears in Exhibit F attached to the Complaint. Defendants lack sufficient information to admit or deny the remaining allegations in this Paragraph and, therefore, deny the same.

41. Further, as of July 28, 2016, Windows 10 requires all new devices to implement and enable by default TPM 2.0:

## TPM 2.0 Compliance for Windows 10

### Windows 10 for desktop editions (Home, Pro, Enterprise, and Education)

- Since July 28, 2016, all new device models, lines or series (or if you are updating the hardware configuration of a existing model, line or series with a major update, such as CPU, graphic cards) must implement and enable by default TPM 2.0 (details in section 3.7 of the [Minimum hardware requirements](#) page). The requirement to enable TPM 2.0 only applies to the manufacturing of new devices. For TPM recommendations for specific Windows features, see [TPM and Windows Features](#).

See Exhibit G, TPM Recommendations at “TPM 2.0 Compliance for Windows 10” (available at <https://docs.microsoft.com/en-us/windows/security/information-protection/tpm/tpm-recommendations>, last visited June 29, 2021).

**ANSWER:** Defendants admit that the screenshotted image without a red line annotation appears in Exhibit G attached to the Complaint. Defendants lack sufficient information to admit or deny the remaining allegations in this Paragraph and, therefore, deny the same.

42. Therefore, the Accused Instrumentalities meet limitation B1 of claim 19.

**ANSWER:** Denied.

43. Limitation B2 requires that “detecting the insecure condition includes” “receiving a response and determining whether the response includes a valid digitally signed attestation of cleanliness.” The Accused Instrumentalities also meet all the requirements of limitation B2 of claim 19. For example, whenever the OnGuard needs health information, it informs the Backend Service, which collects the health information and sends a Statement of Health (SoH) back to the OnGuard Plugin. *See* Exhibit E, ClearPass OnGuard Troubleshooting at 47. Accordingly, each health check returns an application token representing health:

#### **Application Token**

Each configured health check returns an application token representing health:

- **Healthy.** Client is compliant: there are no restrictions on network access.
- **Checkup.** Client is compliant; however, there is an update available. This can be used to proactively remediate to healthy state.
- **Transient.** Client evaluation is in progress; typically associated with auditing a client. The network access granted is interim.
- **Quarantine.** Client is out of compliance; restrict network access so the client only has access to the remediation servers.
- **Infected.** Client is infected and is a threat to other systems in the network; network access should be denied or severely restricted.
- **Unknown.** The posture token of the client is unknown.

See Exhibit H, Posture Architecture and Flow at 2 (available at [https://www.arubanetworks.com/techdocs/ClearPass/6.8/PolicyManager/index.htm#CPPM\\_UserGuide/Posture/postureArchandFlow.html%3FTocPath%3DPosture%2520Policies%252C%2520Audit%2520Servers%252C%2520Agentless%2520OnGuard%7C\\_\\_1](https://www.arubanetworks.com/techdocs/ClearPass/6.8/PolicyManager/index.htm#CPPM_UserGuide/Posture/postureArchandFlow.html%3FTocPath%3DPosture%2520Policies%252C%2520Audit%2520Servers%252C%2520Agentless%2520OnGuard%7C__1), last visited July 8, 2021). The ClearPass Policy Manager then evaluates all application tokens and calculates a system token that is equivalent to the most restrictive rating for all returned application tokens. *See id.*

**ANSWER:** Defendants admit that the quoted text in Paragraph 43 appears in claim 19 of the '705 Patent. Defendants admit that the screenshotted image appears in Exhibit H attached to the Complaint. Defendants lack sufficient information to admit or deny the remaining allegations in this Paragraph and, therefore, deny the same.

44. Thus, the Accused Instrumentalities meet limitation B2 of claim 19.

**ANSWER:** Denied.

45. Limitation C requires that “the valid digitally signed attestation of cleanliness includes at least one of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host.” The Accused Instrumentalities also meets all the requirements of limitation C of claim 19. For example, OnGuard performs the following posture and health checks:

	Windows	macOS	Linux
Installed Applications	X	X	
AntiVirus	X	X	X
Firewall	X	X	
Disk Encryption	X	X	
Network Connections	X	X	
Processes	X	X	
Patch Management	X	X	
Peer to Peer	X	X	
Services	X	X	X
Virtual Machines	X	X	
Windows Hotfixes	X		
USB Devices	X	X	
File Check	X	X	

\* Chart represents ClearPass version 6.8 functionality.

\*\* Disclaimer: Not all checks are supported across operating systems and agent type.

See Exhibit D, Data Sheet HPE Aruba ClearPass OnGuard at 2.

**ANSWER:** Defendants admit that the quoted text in Paragraph 45 appears in claim 19 of the '705 Patent. Defendants admit that the screenshotted image appears in Exhibit D attached to the Complaint. Defendants lack sufficient information to admit or deny the remaining allegations in this Paragraph and, therefore, deny the same.

46. Accordingly, the Accused Instrumentalities meet limitation C of claim 19.

**ANSWER:** Denied.

47. Limitation D requires that “when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network.” The Accused Instrumentalities also meets all the requirements of limitation D of claim 19. For example, each health check returns an application token representing health, including a token of “Quarantine” that indicates that the client is out of compliance and to restrict network access so the client only has access to the remediation servers. See Exhibit H, Posture Architecture and Flow at 2. Accordingly, the Accused Instrumentalities meet limitation D of claim 19.

**ANSWER:** Defendants admit that the quoted text in Paragraph 47 appears in claim 19 of the '705 Patent. Defendants lack sufficient information to admit or deny the remaining allegations in this Paragraph and, therefore, deny the same.

48. Limitation E1 requires that “preventing the first host from sending data to one or more other hosts associated with the protected network includes” “receiving a service request sent by the first host [and] serving a quarantine notification page to the first host when the service request comprises a web server request.” The Accused Instrumentalities also meets all the requirements of limitation E1 of claim 19. For example, when using a web-based dissolvable

Posture Settings	
Enable Posture Checks	Select the check box to perform health checks post authentication. This enables the <b>Host Operating System</b> and <b>Quarantine Message</b> fields.
Host Operating System	Select the operating system: Windows, Linux, or macOS.
Quarantine Message	Specify the quarantine message that will appear on the client.
Initial Role/ VLAN	Enter the initial role of the client before posture checks are performed.
Quarantine Role/VLAN	Enter the role of clients that fail posture checks.

ClearPass OnGuard agent, a one-time check at login ensures policy compliance. *See* Exhibit D, Data Sheet HPE Aruba ClearPass OnGuard at 2. Further, non-compliant devices can be redirected to a captive portal for remediation. *See id.* For example, the ClearPass Policy Manager provides a Guest Access Service Template designed for guest users who log in using captive portal. *See* Exhibit I, Guest Access Service Template (available at [https://www.arubanetworks.com/techdocs/ClearPass/6.7/PolicyManager/Content/CPPM\\_UserGuide/Services/ServiceTemplates\\_Guest.htm](https://www.arubanetworks.com/techdocs/ClearPass/6.7/PolicyManager/Content/CPPM_UserGuide/Services/ServiceTemplates_Guest.htm), last visited July 9, 2021). Moreover, posture checks can be enabled along with a quarantine message that will appear on the client.

**ANSWER:** Defendants admit that the quoted text in Paragraph 48 appears in claim 19 of the '705 Patent. Defendants admit that the screenshotted image appears in Exhibit I attached to the Complaint. Defendants lack sufficient information to admit or deny the remaining allegations in this Paragraph and, therefore, deny the same.

49. Accordingly, the Accused Instrumentalities meet limitation E1 of claim 19.

**ANSWER:** Denied.

50. Limitation E2 requires that “preventing the first host from sending data to one or more other hosts associated with the protected network includes” “in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server configured to serve the quarantine notification page if a host name that is the subject of the DNS query is not associated with a remediation host configured to provide data usable to remedy the insecure condition.” The Accused Instrumentalities also meets all the requirements of limitation E2 of claim 19. For example, when using a web-based dissolvable ClearPass OnGuard agent, a one-time check at login ensures policy compliance. *See* Exhibit D, Data Sheet HPE Aruba ClearPass OnGuard at 2. Further, non-compliant devices can be redirected to a captive portal for remediation. *See id.* Accordingly, the Accused Instrumentalities meet limitation E2 of claim 19.

**ANSWER:** Defendants admit that the quoted text in Paragraph 50 appears in claim 19 of the '705 Patent. Defendants lack sufficient information to admit or deny the remaining allegations in this Paragraph and, therefore, deny the same.

51. Limitation F requires “permitting the first host to communicate with the remediation host.” The Accused Instrumentalities also meets all the requirements of limitation F of claim 19. For example, each health check returns an application token representing health, including a token of “Quarantine” that indicates that the client is out of compliance and to restrict network access so the client only has access to the remediation servers. *See* Exhibit H, Posture

Architecture and Flow at 2. Accordingly, the Accused Instrumentalities meet limitation F of claim 19.

**ANSWER:** Defendants admit that the quoted text in Paragraph 51 appears in claim 19 of the '705 Patent. Defendants lack sufficient information to admit or deny the remaining allegations in this Paragraph and, therefore, deny the same.

52. Accordingly, on information and belief, the Accused Instrumentalities meet all the limitations of, and therefore infringe, at least claim 19 of the '705 patent.

**ANSWER:** Denied.

53. As a result of Aruba's infringement of the '705 patent, K.Mizra has suffered and continues to suffer substantial injury and is entitled to recover all damages caused by Aruba's infringement to the fullest extent permitted by the Patent Act, together with prejudgment interest and costs for Aruba's wrongful conduct.

**ANSWER:** Denied.

54. K.Mizra re-alleges and incorporates by reference all of the foregoing paragraphs.

**ANSWER:** Defendants incorporate by reference their answers to Paragraphs 1 through 53 as if fully set forth herein.

55. On information and belief, K.Mizra has infringed and continues to infringe, either literally or under the doctrine of equivalents, one or more claims, including at least claim 17, of the '048 patent in violation of 35 U.S.C. §§ 271 et seq., by making, using, importing, selling, offering for sale, and/or importing in this District and into the United States certain products including, but not limited to those, relating to the Accused Instrumentalities.

**ANSWER:** Defendants lack sufficient information to admit or deny the allegations in this Paragraph and, therefore, deny the same.

56. For example, Claim 17 of the '048 patent recites the following:

[preamble] A computer program product for protecting a network, the computer program product being embodied in a non-transitory computer readable medium and comprising instructions for:

[A] detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network,

[B] wherein detecting the insecure condition includes

[B1] contacting a trusted computing base associated with a trusted platform module within the first host,

[B2] receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness,

[C] wherein the valid digitally signed attestation of cleanliness includes at least one attestation elected from the group consisting of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host;

[D] when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network,

[E] wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes

[E1] receiving a service request sent by the first host, determining whether service request sent by the first host is associated with a remediation request, and when it is determined that the service request sent by the first host is associated with a remediation request, serving a quarantine notification page that provides remediation information to the first host if the service request sent by the first host comprises a web server request

[E2] wherein serving the quarantine notification page to the first host includes re-routing by responding to the service request by the first host to be directed to a quarantine server configured to serve the quarantine notification page; and

[F] permitting the first host to communicate with the remediation host configured to provide data usable to remedy the insecure condition.

**ANSWER:** Denied.

57. On information and belief, and based on publicly available information, at least the Accused Instrumentalities satisfy each and every limitation of at least claim 17 of the '048 patent.

**ANSWER:** Denied.

58. The preamble recites a “computer program product for protecting a network.” Regarding the preamble of claim 17, to the extent the preamble is determined to be limiting, the Accused Instrumentalities provide the features described in the preamble. *See, e.g., supra* ¶¶ 33-34 ('705 patent preamble analysis). Thus, to the extent the preamble of claim 17 is limiting, the Accused Instrumentalities meet it.

**ANSWER:** Denied.

59. Limitation A recites “detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network.” The Accused Instrumentalities also meet all the requirements of limitation A of claim 17. *See, e.g., supra* ¶ 35 ('705 patent Limitation A analysis). Thus, the Accused Instrumentalities meet limitation A of claim 17.

**ANSWER:** Defendants admit that the quoted text in Paragraph 59 appears in claim 17 of the '048 Patent. Defendants lack sufficient information to admit or deny the remaining allegations in this Paragraph and, therefore, deny the same.

60. Limitation B1 recites “wherein detecting the insecure condition includes” “contacting a trusted computing base associated with a trusted platform module within the first host.” The Accused Instrumentalities also meet all the requirements of limitation B1 of claim 17. *See, e.g., supra* ¶¶ 36-39 ('705 patent Limitation B1 analysis). Thus, the Accused Instrumentalities meet limitation B1 of claim 17.

**ANSWER:** Defendants admit that the quoted text in Paragraph 60 appears in claim 17 of the '048 Patent. Defendants lack sufficient information to admit or deny the remaining allegations in this Paragraph and, therefore, deny the same.

61. Limitation B2 recites “wherein detecting the insecure condition includes” “receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness.” The Accused Instrumentalities also meet all the requirements of limitation B2 of claim 17. *See, e.g., supra* ¶¶ 40-41 ('705 patent Limitation B2 analysis). Thus, the Accused Instrumentalities meet limitation B2 of claim 17.

**ANSWER:** Defendants admit that the quoted text in Paragraph 61 appears in claim 17 of the '048 Patent. Defendants lack sufficient information to admit or deny the remaining allegations in this Paragraph and, therefore, deny the same.

62. Limitation C recites “wherein the valid digitally signed attestation of cleanliness includes at least one attestation elected from the group consisting of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host.” The Accused Instrumentalities also meet all the requirements of limitation C of claim 17. *See, e.g., supra* ¶¶ 42-43 ('705 patent Limitation C analysis). Thus, the Accused Instrumentalities meet limitation C of claim 17.

**ANSWER:** Defendants admit that the quoted text in Paragraph 62 appears in claim 17 of the '048 Patent. Defendants lack sufficient information to admit or deny the remaining allegations in this Paragraph and, therefore, deny the same.

63. Limitation D recites “when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network.” The Accused Instrumentalities also meet all the requirements of limitation D of claim 17. *See, e.g., supra* ¶ 44 ('705 patent Limitation D analysis). Thus, the Accused Instrumentalities meet limitation D of claim 17.

**ANSWER:** Defendants admit that the quoted text in Paragraph 63 appears in claim 17 of the '048 Patent. Defendants lack sufficient information to admit or deny the remaining allegations in this Paragraph and, therefore, deny the same.

64. Limitation E1 recites “wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes” “receiving a service request sent by the first host, determining whether service request sent by the first host is associated with a remediation request, and when it is determined that the service request sent by the first host is associated with a remediation request, serving a quarantine notification page that provides remediation information to the first host if the service request sent by the first host comprises a web server request.” The Accused Instrumentalities also meet all the requirements of limitation E1 of claim 17. *See, e.g., supra* ¶¶ 45-46 ('705 patent Limitation E1 analysis). Thus, the Accused Instrumentalities meet limitation E1 of claim 17.

**ANSWER:** Denied.

65. Limitation E2 recites “wherein serving the quarantine notification page to the first host includes re-routing by responding to the service request by the first host to be directed to a quarantine server configured to serve the quarantine notification page.” The Accused Instrumentalities also meet all the requirements of limitation E2 of claim 17. *See, e.g., supra* ¶ 47 (‘705 patent Limitation E2 analysis). Thus, the Accused Instrumentalities meet limitation E2 of claim 17.

**ANSWER:** Denied.

66. Limitation F recites “permitting the first host to communicate with the remediation host configured to provide data usable to remedy the insecure condition.” The Accused Instrumentalities also meet all the requirements of limitation F of claim 17. *See, e.g., supra* ¶¶ 48-49 (‘705 patent Limitation F analysis). Thus, the Accused Instrumentalities meet limitation F of claim 17.

**ANSWER:** Defendants admit that the quoted text in Paragraph 66 appears in the ‘048 Patent. Defendants lack sufficient information to admit or deny the remaining allegations in this Paragraph and, therefore, deny the same.

67. Accordingly, on information and belief, the Accused Instrumentalities meet all the limitations of, and therefore infringe, at least claim 17 of the ‘048 patent.

**ANSWER:** Denied.

68. As a result of K.Mizra’s infringement of the ‘048 patent, K.Mizra has suffered and continues to suffer substantial injury and is entitled to recover all damages caused by K.Mizra’s infringement to the fullest extent permitted by the Patent Act, together with prejudgment interest and costs for K.Mizra’s wrongful conduct.

**ANSWER:** Defendants lack sufficient information to admit or deny the allegations in this Paragraph and, therefore, deny the same.

Defendants deny that K.Mizra is entitled to any relief from Defendants, much less the relief set forth in K.Mizra’s Prayer for Relief, at least because the claims of the ‘705 and ‘048 Patents are neither valid, enforceable, nor infringed, either directly or indirectly, by Defendants. Defendants deny all of the allegations in K.Mizra’s Prayer for Relief.

Defendants deny each allegation in the Complaint to which they do not specifically admit above.

### **AFFIRMATIVE DEFENSES**

Without assuming any burden of production or proof that they would not otherwise be required to bear under applicable law, and reserving their right to assert additional defenses and/or affirmative defenses, Defendants assert the following affirmative defenses:

#### **FIRST AFFIRMATIVE DEFENSE**

Plaintiff has failed to state a claim upon which relief can be granted.

#### **SECOND AFFIRMATIVE DEFENSE**

K.Mizra lacks standing to sue for infringement as the rightful owner of the Patents-in-Suit.

#### **THIRD AFFIRMATIVE DEFENSE**

Defendants do not infringe, and have not infringed, any claim of the Patents-in-Suit, literally, directly, indirectly, contributorily, by way of inducement, and/or under the doctrine of equivalents.

#### **FOURTH AFFIRMATIVE DEFENSE**

The claims of the Patents-in-Suit are invalid for failure to meet the requirements of the Patent Act, 35 U.S.C. § 1 *et seq.*, including, but not limited to, one or more of 35 U.S.C. §§ 101, 102, 103, and/or 112.

#### **FIFTH AFFIRMATIVE DEFENSE**

By reason of the proceedings in the U.S. Patent and Trademark Office during the prosecution of the application resulting in the issuance of the Patents-in-Suit, Plaintiff is estopped from claiming infringement by Defendants of one or more claims of the Patents-in-Suit.

**SIXTH AFFIRMATIVE DEFENSE**

Plaintiff's claims for patent infringement are precluded in whole or in part: (i) to the extent any allegedly infringing products are supplied, directly or indirectly, to Defendants by an entity or entities having express or implied licenses to the Patents-in-Suit; and/or (ii) under the doctrine of patent exhaustion.

**SEVENTH AFFIRMATIVE DEFENSE**

Any claim by Plaintiff for damages is limited under 35 U.S.C. §§ 286 or 287. Plaintiff is barred under 35 U.S.C. § 287 from recovering damages before the filing of its Complaint. Plaintiff is further barred by 35 U.S.C. § 288 from recovering costs associated with its action.

**EIGHTH AFFIRMATIVE DEFENSE**

Plaintiff is barred, in whole or in part, under principles of equity, including prosecution laches, acquiescence, express and/or implied license, waiver, estoppel, unclean hands, and/or any other equitable remedy. Plaintiff is also barred by issue preclusion from reasserting or altering its, or its predecessor-in-interest's, positions on factual and legal issues that were previously adjudicated.

**NINTH AFFIRMATIVE DEFENSE**

Any claim by Plaintiff for increased damages due to alleged willful infringement of the Patents-in-Suit is improper as Plaintiff cannot show that Defendants knew or should have known that their actions constituted infringement of a valid claim of the Patents-in-Suit or otherwise meet the requirements for willful infringement.

**TENTH AFFIRMATIVE DEFENSE**

Defendants have an implied or express license to the Patents-in-Suit.

### **RESERVATION OF RIGHTS**

Defendants hereby give notice that they intend to rely upon any other defense that may become available or appear during the discovery proceedings in this case and reserve the right to amend their Answer and Affirmative Defenses to assert any such defense.

### **DEMAND FOR JURY TRIAL**

Defendants request a jury trial on all issues so triable.

### **HEWLETT PACKARD ENTERPRISE COMPANY AND ARUBA NETWORK LLC'S COUNTERCLAIMS**

Pursuant to Rule 13 of the Federal Rules of Civil Procedure, Hewlett Packard Enterprise Company ("HPE") and Aruba Networks, LLC ("Aruba") (collectively, "Defendants") assert the following Counterclaims against K.Mizra LLC ("K.Mizra" or "Plaintiff"). Defendants reserve the right to amend their Counterclaims to assert additional claims which may be revealed during discovery.

### **NATURE AND BASIS OF ACTION**

1. This is an action arising under the Declaratory Judgment Act, 28 U.S.C. §§ 2201 and 2202, and the United States Patent Act, 35 U.S.C. § 1 et seq. Defendants respectfully request declarations that: (i) they do not infringe any valid, enforceable claim of U.S. Patent Nos. 8,234,705 ("the '705 patent") and 9,516,048 ("the '048 patent"), also referred to as "the Patents-in-Suit"; and (ii) the claims of the Patents-in-Suit are invalid.

### **THE PARTIES**

2. HPE is a Delaware Corporation having its principal place of business at 11445 Compaq Center West Drive, Houston, Texas 77070.

3. Aruba Networks, LLC (“Aruba”) is a limited liability company organized and existing under the laws of Delaware having its principal place of business at 6280 America Center Drive, San Jose, California 95002.

4. According to Plaintiff’s Complaint, K.Mizra is a Delaware limited liability company with its principal place of business at 777 Brickell Ave, #500-96031, Miami, FL 33131.

### **JURISDICTION AND VENUE**

5. Subject to Defendants’ defenses and denials, this Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. §§ 1331 and 1338, and the Declaratory Judgment Act, 28 U.S.C. §§ 2201 and 2202. This Court also has supplemental jurisdiction over Defendants’ Fifth Counterclaim under 28 U.S.C. § 1367.

6. Subject to Defendants’ defenses and denials, and any request to seek transfer of venue under 28 U.S.C. § 1404(a), personal jurisdiction and venue are proper in this District under at least 28 U.S.C. §§ 1391(b), 1391(c), and 1400(b), because, among other reasons, Plaintiff has submitted to the venue of this Court by filing its Complaint here.

### **FACTUAL ALLEGATIONS**

7. According to Plaintiff’s Complaint, K.Mizra purports to be the owner of the Patents-in-Suit.

8. Defendants do not infringe directly or indirectly, by inducement or by contribution, any valid, enforceable claim of the Patents-in-Suit.

9. Upon information and belief, all claims of the Patents-in-Suit are invalid for failure to meet the requirements of the Patent Act, 35 U.S.C. § 1 *et seq.*, including, but not limited to, 35 U.S.C. §§ 101, 102, 103, and/or 112.

10. HPE and K.Mizra executed a Mutual Confidentiality and Standstill Agreement (“Standstill Agreement”) on February 5, 2021, attached hereto as Exhibit 1.

11. The stated “Purpose” of the Standstill Agreement is defined as “a discussion regarding the licensing of the patents.” Exhibit 1 at preamble.

12. Under the Standstill Agreement, the parties agreed that neither party would disclose:

(b) the fact that discussions or negotiations may be, or are, underway between the Parties regarding the Confidential Information or the Purpose, including the status thereof;

Exhibit 1 at ¶ 4(b).

13. Under the Standstill Agreement, the parties further agreed that neither disclosure nor receipt of “Confidential Information” under the Agreement:

“shall constitute, or be used by either Party, or any successor-interest, as evidence in any legal proceeding to prove or disprove: (a) notice of infringement received by Recipient during a Discussion Period; (b) direct or indirect infringement; (c) damages based on reasonably royalties, lost profits, or any other remedy or theory of liability; or (d) enhanced damages based on (a).

Exhibit 1 at ¶ 5.

14. In its Complaint against HPE and Aruba, K.Mizra made allegations disclosing the receipt of Confidential Information by HPE during negotiations under the Standstill Agreement and the status of those negotiations. *See* Compl. at ¶¶ 10-11.

15. In its Complaint against HPE and Aruba, K.Mizra seeks a finding that HPE and Aruba’s alleged infringement has been willful as to the ’705 Patent based on the parties’ negotiations commencing in January 2021. *See* Compl. at Prayer for Relief, ¶ D.

**FIRST COUNTERCLAIM**  
**(DECLARATORY JUDGMENT OF NON-INFRINGEMENT OF THE '705 PATENT)**

16. Defendants reallege and reincorporate the allegations of Paragraphs 1 through 15, inclusive, of their Counterclaims as if set forth here in full.

17. Defendants have not infringed and do not directly or indirectly infringe (such as by inducement or contributory infringement) any valid and enforceable claim of the '705 Patent and have not otherwise committed any acts of patent infringement in violation of 35 U.S.C. § 271.

18. An actual case and controversy exist between Defendants and K.Mizra based on K.Mizra having filed the Complaint against Defendants alleging infringement of the '705 Patent.

19. Defendants have been injured and damaged by K.Mizra's lawsuit.

20. Defendants therefore seek a declaration that they have not infringed, and do not directly or indirectly infringe, literally or under the doctrine of equivalents, any valid and enforceable claim of the '705 Patent.

**SECOND COUNTERCLAIM**  
**(DECLARATORY JUDGMENT OF INVALIDITY OF THE '705 PATENT)**

21. Defendants reallege and reincorporate the allegations of Paragraphs 1 through 20, inclusive, of their Counterclaims as if set forth here in full.

22. The claims of the '705 Patent are invalid for failing to meet the conditions for patentability in 35 U.S.C. § 1 *et seq.*, including §§ 101, 102, 103, and/or 112.

23. The claims of the '705 Patent are invalid under § 112 for failure to enable and provide adequate written description for the claimed invention and because the claims do not particularly point out and distinctly claim the subject matter which the inventor regards as the invention.

24. The claims of the '705 Patent are invalid under § 101 for being directed to an unpatentable abstract idea, and for failing to recite an inventive concept. *Alice Corp. Pty. v. CLS Bank Int'l*, 573 U.S. 208, 216 (2014).

25. The claims of the '705 Patent are also invalid as anticipated and/or rendered obvious by at least, *inter alia*, U.S. Patent No. 9,436,820 to Gleichauf et al., U.S. Patent No. 7,747,862 to Ovadia, and U.S. Patent No. 7,533,407 to Lewis et al.

26. An actual controversy exists between Defendants and K.Mizra based on K.Mizra having filed the Complaint against Defendants alleging infringement of the '705 Patent.

27. Defendants have been injured and damaged by K.Mizra's lawsuit.

28. Defendants therefore seek a declaration that the '705 Patent is invalid for failing to meet the conditions for patentability in 35 U.S.C. § 1 *et seq.*

**THIRD COUNTERCLAIM**  
**(DECLARATORY JUDGMENT OF NON-INFRINGEMENT OF THE '048 PATENT)**

29. Defendants reallege and reincorporate the allegations of Paragraphs 1 through 28, inclusive, of their Counterclaims as if set forth here in full.

30. Defendants have not infringed and does not directly or indirectly infringe (such as by inducement or contributory infringement) any valid and enforceable claim of the '048 Patent and have not otherwise committed any acts of patent infringement in violation of 35 U.S.C. § 271.

31. An actual case and controversy exist between Defendants and K.Mizra based on K.Mizra having filed the Complaint against Defendants alleging infringement of the '048 Patent.

32. Defendants have been injured and damaged by K.Mizra's lawsuit.

33. Defendants therefore seek a declaration that they have not infringed, and do not directly or indirectly infringe, literally or under the doctrine of equivalents, any valid and enforceable claim of the '048 Patent.

**FOURTH COUNTERCLAIM**  
**(DECLARATORY JUDGMENT OF INVALIDITY OF THE '048 PATENT)**

34. Defendants reallege and reincorporate the allegations of Paragraphs 1 through 33, inclusive, of their Counterclaims as if set forth here in full.

35. The claims of the '048 Patent are invalid for failing to meet the conditions for patentability in 35 U.S.C. § 1 *et seq.*, including §§ 101, 102, 103, and/or 112, for at least the reasons provided below.

36. The claims of the '048 Patent are invalid under § 112 for failure to enable and provide adequate written description for the claimed invention and because the claims do not particularly point out and distinctly claim the subject matter which the inventor regards as the invention.

37. The claims of the '048 Patent are invalid under § 101 for being directed to an unpatentable abstract idea, and for failing to recite an inventive concept. *Alice Corp. Pty. v. CLS Bank Int'l*, 573 U.S. 208, 216 (2014).

38. The claims of the '048 Patent are also invalid as anticipated and/or rendered obvious by at least, *inter alia*, U.S. Patent No. 9,436,820 to Gleichauf *et al.*, U.S. Patent No. 7,747,862 to Ovadia, and U.S. Patent No. 7,533,407 to Lewis *et al.*

39. An actual controversy exists between Defendants and K.Mizra based on K.Mizra having filed the Complaint against Defendants alleging infringement of the '048 Patent.

40. Defendants have been injured and damaged by K.Mizra's lawsuit.

41. Defendants therefore seek a declaration that the '048 Patent is invalid for failing to meet the conditions for patentability in 35 U.S.C. § 1 *et seq.*

**FIFTH COUNTERCLAIM**  
**(BREACH OF CONTRACT)**

42. Defendants reallege and reincorporate the allegations of Paragraphs 1 through 41, inclusive, of their Counterclaims as if set forth here in full.

43. HPE and K.Mizra are parties to the Standstill Agreement.

44. The Standstill Agreement is a valid and enforceable contract.

45. K.Mizra is bound by the provisions of the Standstill Agreement.

46. At all times, HPE has met its contractual obligations under the Standstill Agreement.

47. As alleged above, K.Mizra agreed not to disclose information regarding negotiations between the parties under the Standstill Agreement. K. Mizra further agreed that neither disclosure nor receipt of “Confidential Information” during those negotiations would be used as evidence of notice of infringement, infringement, or damages.

48. In its Complaint, K.Mizra disclosed information regarding the status and Purpose of the parties’ negotiations and further made such allegations in support of claims to notice of infringement, infringement, and damages.

49. In light of the above-alleged disclosures, K.Mizra has breached its contractual obligations under the Standstill Agreement.

50. HPE is entitled to recover damages resulting from K.Mizra’s breach of its contractual obligations under the Standstill Agreement.

51. HPE has been, and will continue to be, damaged by K.Mizra’s breach of the Standstill Agreement.

**REQUEST FOR RELIEF**

WHEREFORE, Defendants respectfully request a judgment as follows:

- A. that the Court dismiss with prejudice Plaintiff's Complaint;
- B. that the Court deny Plaintiff any relief against Defendants;
- C. that the Court enter a judgment that the '705 Patents is invalid;
- D. that the Court enter a judgment that the '048 Patent is invalid;
- E. that the Court enter a judgment that Defendants do not infringe any claim of the '705 Patent;
- F. that the Court enter a judgment that Defendants do not infringe any claim of the '048 Patent;
- G. that the Court enter a judgment that K.Mizra has breached the Standstill Agreement, causing harm to HPE in an amount to be determined by a jury;
- H. that the Court declare this is an exceptional case under 35 U.S.C. § 285 and award Defendants their costs and attorneys' fees; and
- I. that the Court award Defendants any and all other relief to which they may be entitled, or which the Court deems just and proper.

### **JURY DEMAND**

In accordance with Rule 38 of the Federal Rules of Civil Procedure, Defendants respectfully demand a jury trial of all issues triable to a jury in this action.

Respectfully submitted,

/s/ Joshua R. Thane

Joshua R. Thane

Texas Bar No. 24060713

Kyle R. Akin

Texas Bar No. 24105422

HALTOM & DOAN

6500 Summerhill Road, Suite 100

Texarkana, TX 75503

Telephone: (903) 255-1000

Facsimile: (903) 255-0800

Email: jthane@haltomdoan.com

Email: kakin@haltomdoan.com

Hersh Mehta

IL Bar No. 6306586

Cristina Q. Almendarez

IL Bar No. 6316733

BENESCH FRIEDLANDER COPLAN &

ARONOFF LLP

71 South Wacker Drive, Suite 1600

Chicago, IL 60606 4637

Telephone: (312) 624-6403

Facsimile: (312) 767-9192

hmehta@beneschlaw.com

calmendarez@beneschlaw.com

**ATTORNEY FOR DEFENDANTS  
HEWLETT-PACKARD ENTERPRISE  
COMPANY AND ARUBA NETWORKS,  
LLC**

**CERTIFICATE OF SERVICE**

The undersigned certifies all counsel of record are being served with a copy of this document via electronic mail on this the 15th day of October, 2021.

/s/ Kyle R. Akin

Kyle R. Akin